benefitspro

May 22, 2014

Fast-rising medical ID theft hits employers hard

By: Alan GoForth

About the last thing companies dealing with the complexities of implementing Obamacare need right now is to have the security of their employees' medical information compromised. However, statistics show that is exactly what is happening.

"Medical identity theft is a rapidly spreading malady, often by organized-crime rings," said James Quiggle, spokesman for the Coalition Against Insurance Fraud, a nonprofit alliance of carriers, consumer groups and government agencies in Washington, D.C. "Data breaches in this era of digital record-keeping can drain businesses and make employee records as vulnerable as patients."

More than 1.8 million Americans were victims of medical identity theft in 2013, a crime that is increasing at an annual rate of 32 percent. This makes it the fastest-growing type of identity theft, according to the Identity Theft Resource Center in San Diego.

Medical ID theft is already a multibillion-dollar industry. For the fiscal year ending Sept. 30, 2013, the federal government alone recovered a record $4.3 billion from people and companies that attempted to defraud health-care programs, according to the U.S. Department of Justice and the U.S. Department of Health and Human Services.

Stealing enough personal information to purchase services or devices is not difficult for a sophisticated identity thief, said Drew Smith, founder and CEO of Scottsdale, Ariz.-based InfoArmor. His company has provided B-to-B clients with protection against various types of ID theft since 2007.

"You can go online and readily purchase someone's basic identity information for about $50," he said. "You usually don't need a lot of identification to receive medical care. Most identity thieves are not using it for primary care. It's going for things such as medical devices, prescription drugs or other areas where there is less likely to be a personal relationship with the provider."

Hidden employer costs

Statistics rarely account for the hidden cost of lost productivity when an employee has been victimized. Dealing with the fallout can be a painstaking, time-consuming process. The average medical identity theft loss is $22,346 – six times higher than financial identity theft. Also, on average, it takes victims more than a year to clear up medical records and repair any damage to their credit.

"Employees have to deal with identity theft issues immediately, which requires time off work and lost productivity, because some banks and agencies may be open only on work days," Smith said. "Most medical ID thefts go undetected for a year. It's not like credit card fraud, where you usually are notified quickly if someone tries to use a stolen card. Because of the way medical records are stored, they are extremely fragmented and hard to fix when you find out. That's why reducing the risk of medical identification theft can help a business's bottom line."

Employers may be surprised to learn that medical identity theft may be as likely to occur from within their organization as from outside.

"Fifty percent of medical ID claims are considered `friendly fraud'," Smith said. "For example, an employee's brother may be out of work and they allow him to use their insurance card, or a family member borrows it without permission."

Best defenses

Although eliminating medical ID theft may be impossible, businesses do have effective options to significantly reduce risks and quickly detect breaches. "Managers must implant internal controls and train employees to harden their protection of personal data," Quiggle said. "Protocols to protect against insider theft are especially important."

View the entire article. View other articles quoting the Coalition Against Insurance Fraud.